

FEDERAL PUBLIC DEFENDER
NORTHERN DISTRICT OF CALIFORNIA
13TH FLOOR FEDERAL BUILDING - SUITE 1350N
1301 CLAY STREET
OAKLAND, CA 94612

STEVEN G. KALAR
Federal Public Defender
HANNI M. FAKHOURY
Assistant Federal Public Defender

FILED
AUG 16 2019
SUSAN Y. SOONG
CLERK U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE

Telephone: (510) 637-3500
Fax: (510) 637-3507
Email: Hanni_Fakhoury@fd.org

5-19-71283-VK1

August 9, 2019

DELIVERED VIA EMAIL TO: VKDCRD@CAND.USCOURTS.GOV

The Honorable Virginia K. DeMarchi
United States Magistrate Judge
San Jose Courthouse, Courtroom 2 - 5th Floor
280 South 1st Street
San Jose, CA 95113

SEALED BY ORDER
OF COURT

RE: Fourth & Fifth Amendment Implications of Compelling a Suspect to Unlock an Electronic Device With a Biometric

Your Honor:

Thank you for allowing the Federal Public Defender to provide the Court with its position on the Fourth and Fifth Amendment implications of compelling a suspect to use biometric features, such as a thumbprint, to unlock an electronic device.

It is our position that the Fourth Amendment requires probable cause not only that a specified electronic device has evidence of criminal activity on it, but also that it belongs to a specific suspect before that person can be compelled to unlock the device with biometrics, such as a fingerprint. Law enforcement requests to compel "any individual" at the premises of a search to provide biometrics to unlock "any" unspecified device are not particularized and overbroad in violation of the Fourth Amendment.

As to the Fifth Amendment, the act of compelling a person to unlock an electronic device with a biometric is a "testimonial" act that implicates the privilege against self-incrimination. The "foregone conclusion" doctrine, which withholds Fifth Amendment protection for specific documents the government already knows exist and possessed by the suspect, requires a comprehensive showing of "reasonable particularity" that specific data exists in a specific location, is possessed by the target, and is authentic. The only way the government can overcome the privilege is by offering a suspect both use and derivative use immunity.

4th & 5th Amendment Implications of Compelled Biometric Unlocking
August 9, 2019
Page 2

A. The Fourth Amendment

The Fourth Amendment states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. AMEND. IV. The Fourth Amendment “is informed by historical understandings ‘of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted.’” *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) (quoting *Carroll v. United States*, 267 U.S. 132, 149 (1925)). It “seeks to secure ‘the privacies of life’ against ‘arbitrary’ power.” *Id.* (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). Indeed, the “central aim of the Framers was ‘to place obstacles in the way of a too permeating police surveillance.’” *Id.* (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

A Fourth Amendment “search” occurs when police either physically occupy private property for the purpose of obtaining information, *United States v. Jones*, 565 U.S. 400, 405 (2012), or intrude upon a subjective expectation of privacy that society recognizes as reasonable. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). A legitimate expectation of privacy “must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.” *Rakas v. Illinois*, 439 U.S. 128, 143 n. 12 (1978).

Courts must “assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.” *Kyllo v. United States*, 533 U.S. 27, 34 (2001). But it is also “foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.” *Id.* at 33. The Supreme Court has repeatedly warned that technological changes require critical reexamination of old precedent in modern times to ensure constitutional protections are not “at the mercy of advancing technology.” *Id.* at 35; *see also Carpenter*, 138 S. Ct. at 2223 (lower courts must “ensure that the ‘progress of science’ does not erode Fourth Amendment protections.”) (quoting *Olmstead v. United States*, 277 U.S. 438, 473-74 (1928) (Brandeis, J., dissenting)).

1. Compelling a Suspect to Provide a Biometric, Like a Fingerprint, to Unlock an Electronic Device is a Fourth Amendment “Search.”

As a threshold matter, the government’s act of compelling a person provide a biometric to unlock an electronic device is a Fourth Amendment “search” separate from any subsequent search of the device itself.¹

¹ Following *Riley v. California*, it is unquestionable that people have an objectively reasonable expectation of privacy in their cell phones. *See* 573 U.S. 373, 403 (2014) (cell phones are “worthy of the protection for which the

4th & 5th Amendment Implications of Compelled Biometric Unlocking
 August 9, 2019
 Page 3

A Fourth Amendment “search has undoubtedly occurred” when “the Government obtains information by physically intruding on a constitutionally protected area.” *Jones*, 565 U.S. at 407 n. 3. The Court in *Jones* found police installation of a GPS device onto a car was a Fourth Amendment search. *Id.* at 404-05. In *Grady v. North Carolina*, the Supreme Court extended *Jones* to the placement of a GPS electronic device on a sex offender’s ankle. 135 S. Ct. 1368, 1369 (2015) (per curiam). The Court explained “a State also conducts a search when it attaches a device to a person’s body, without consent, for the purpose of tracking that individual’s movements.” *Id.* at 1370.

Compelling a person to unlock an electronic device with a biometric is identical to the placement of a GPS device on a person’s ankle. In both scenarios, the government is forcing someone to connect their body to an electronic device for the purpose of obtaining large amounts of sensitive, personal information. In *Jones* and *Grady*, the information obtained was a person’s location. In the electronic device scenario, the information sought by the government is the data on the device. Such government action qualifies as a “search” under the Fourth Amendment.

2. The Government Must Have Probable Cause a Specified Electronic Device Contains Evidence of Criminal Activity and Probable Cause the Device is Connected to a Specific Suspect in Order to Compel the Suspect Unlock It With Biometrics.

The government generally needs a particularized search warrant supported by probable cause in order to search a device. That requires the government “establish probable cause to believe [a] crime has been committed and that evidence is likely to be found at the place to be searched.” *Groh v. Ramirez*, 540 U.S. 551, 568 (2004). The government must show a “nexus...between the item to be seized and criminal behavior.” *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 307 (1967).

Multiple Fourth Amendment events must be analyzed separately. Merely obtaining a search warrant for a building does not automatically authorize the seizure of every electronic device found at the premises. *See United States v. Griffith*, 867 F.3d 1265, 1273 (D.C. Cir. 2017) (“it is no answer to confer a blanket authorization to search for and seize all electronic devices.”). Similarly, merely obtaining an arrest warrant for a person does not authorize a search of their cell phone. *See id.* at 1271 (“probable cause to arrest a person will not itself justify a warrant to search his property.”). And as the Supreme Court unanimously held in *Riley*, a lawful arrest is insufficient to justify a warrantless search of data on the arrestee’s cell phone incident to arrest. *See* 573 U.S. at 403.

Thus, when it comes to assessing the constitutionality of “obtaining...physical evidence from a person,” there are “two different levels” of Fourth Amendment analysis. *United States v.*

Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.”); *see also City of Ontario, Cal. v. Quon*, 560 U.S. 746, 760 (2010) (assuming reasonable expectation of privacy in text messages). The Ninth Circuit has also held people have “a legitimate, objectively reasonable expectation of privacy in [their] personal computer.” *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007).

4th & 5th Amendment Implications of Compelled Biometric Unlocking
 August 9, 2019
 Page 4

Dionisio, 410 U.S. 1, 8 (1973). First is “the ‘seizure’ of the ‘person’ necessary to bring him into contact with government agents.” *Id.* Second is “the subsequent search for and seizure of the evidence.” *Id.*

Case law concerning biometrics like fingerprinting, however, have focused on the first issue—the seizure of the person necessary for law enforcement to obtain the biometric—rather than the subsequent search. In *Davis v. Mississippi*, the Supreme Court ruled a detention unsupported by either probable cause or reasonable suspicion for the sole purpose of obtaining a fingerprint violated the Fourth Amendment. 394 U.S. 721, 727 (1969). The Court looked solely at the first “level” of Fourth Amendment analysis—how the fingerprint evidence was obtained—rather than assessing the intrusiveness of obtaining the fingerprint. Indeed, the Court that explained “fingerprinting involves none of the probing into an individual’s private life and thoughts that marks an interrogation or search” and suggested “such detentions might, under narrowly defined circumstances, be found to comply with the Fourth Amendment even though there is no probable cause in the traditional sense.” 394 U.S. at 727–28.

Sixteen years later in *Hayes v. Florida*, the Court explained there is “support in our cases for the view that the Fourth Amendment would permit seizures for the purpose of fingerprinting, if there is reasonable suspicion that the suspect has committed a criminal act, if there is a reasonable basis for believing that fingerprinting will establish or negate the suspect’s connection with that crime, and if the procedure is carried out with dispatch.” 470 U.S. 811, 817 (1985). That was motivated, in part, by the Court’s belief that fingerprinting “represents a much less serious intrusion upon personal security than other types of searches and detentions.” *Id.* at 814.

But as the intrusiveness of the search at the second “level” increases, so must the legal showing necessary to justify that intrusion. See *Matter of Residence in Oakland, California*, 354 F. Supp. 3d 1010, 1017 (N.D. Cal. 2019) (“mobile phones are subject to different treatment than more traditional storage devices, such as safes, and should be afforded more protection.”). Again, the Supreme Court in *Riley* held the mere fact of a lawful arrest—a finding that would satisfy the initial, seizure “level” of Fourth Amendment analysis—was insufficient to satisfy the second “level” of Fourth Amendment analysis: whether the search of data on a cell phone was permitted incident to arrest. As the Court explained, “a conclusion that inspecting the contents of an arrestee’s pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.” *Riley*, 573 U.S. at 393.

Because placing a fingerprint or other biometric in order to unlock an electronic device requires the seizure of a person, is a “search” under *Jones* and *Grady*, and is a much more “serious intrusion” upon personal privacy than the physical act of obtaining a fingerprint, it should have heightened Fourth Amendment protection. As *Riley* makes clear, electronic devices like “modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.” 573 U.S. at 393. “Electronic devices are capable of storing warehouses full of information,” typically “contain[ing] the most intimate details of our lives: financial records, confidential business documents, medical records and private emails.” *United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013) (en banc). Unlocking an electronic device with a biometric necessarily communicates to law enforcement

4th & 5th Amendment Implications of Compelled Biometric Unlocking
 August 9, 2019
 Page 5

that the individual has dominion and control over the electronic device and its contents.² Once law enforcement can link a particular electronic device to a specific person, the government has the ability to “prob[e] into an individual’s private life and thoughts.” *Davis*, 394 U.S. at 727.

Thus, when it comes to compelling a person to provide a biometric to unlock an electronic device, the Fourth Amendment requirement of a “nexus” to criminal behavior means the government must obtain a particularized search warrant supported by probable cause that evidence of criminal activity will be found on the device, and probable cause the device belongs to the person it seeks to compel.

The handful of magistrate judges who have reviewed this specific issue all agree the mere existence of probable cause to search a place is insufficient to also authorize compelling a person provide biometrics to unlock an electronic device found at the premises of the search without a separate and sufficient connection between a specific suspect, and a specified electronic device connected to criminal activity. The courts differ, however, on whether the standard that applies should be probable cause or reasonable suspicion.

In *Matter of Residence in Oakland, California*, the Honorable Kandis A. Westmore found probable cause to authorize the search of a residence in Oakland. 354 F. Supp. 3d at 1013. But she rejected a government request “to compel ‘any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features.’” *Id.* at 1014 (quoting search warrant affidavit).³ Judge Westmore noted the request was unsupported by probable cause and overbroad, as “the request is neither limited to a particular person nor a particular device.” *Id.* She also rejected the government’s “request to search and seize all digital devices” at the premises, finding the request “similarly overbroad.” *Id.* She explained, the “government cannot be permitted to search and seize a mobile phone or other device that is on a non-suspect’s person simply because they are present during an otherwise lawful search.” *Id.*

In *In re Application for a Search Warrant*, the Honorable M. David Weisman found probable cause to authorize the search of a residence in a child pornography investigation. 236 F. Supp.3d 1066, 1067 (N.D. Ill. 2017). But he found the “warrant does not establish sufficient probable cause to compel any person who happens to be at the subject premises at the time of the search to give his fingerprint to unlock an unspecified Apple electronic device.” *Id.* at 1068. He noted the government’s “request is neither limited to a particular person nor a particular device” and “without any specific facts as to who is involved in the criminal conduct linked to the subject

² That is particularly true as biometrics that unlock an electronic device can also be used to log into specific applications on the device, typically those containing sensitive data requiring a separate username or password to access, like banking or messaging applications. *See, e.g.*, “Use Face ID on your iPhone or iPad Pro,” Apple Support, available at <https://support.apple.com/en-us/HT208109> (“You can use Face ID to sign in to apps that support signing in with Touch ID.”) (last visited August 9, 2019).

³ The government appealed Judge Westmore’s decision to the district court, and the appeal is still pending. *See* 4:19-mj-70053-KAW. Notably, the government is the only party to appear in that case and the only party that provided any briefing to the district court.

4th & 5th Amendment Implications of Compelled Biometric Unlocking
 August 9, 2019
 Page 6

premises, or specific facts as to what particular Apple-branded encrypted device is being employed (if any).” *Id.* He had concerns with “the method of obtaining the print”—the first “level” of Fourth Amendment analysis—and did not base his ruling on “the privacy interests of a fingerprint.” *Id.* at 1070.

Conversely, in *Matter of Search of [Redacted] Washington, District of Colombia*, the Honorable G. Michael Harvey found probable cause to search premises tied to a specific suspect, and probable cause that personal electronic devices belonging to the suspect contained evidence about the crime under investigation. 317 F. Supp. 3d 523, 526 (D.D.C. 2018). The government also sought authorization “to attempt to unlock cellphones and computers falling within the scope of the warrant through the compelled use of the Subject’s physical characteristics—*i.e.*, his fingerprints, face, or irises.” *Id.* Judge Harvey framed the issue as “even where the government is permitted to detain briefly an individual during a search warrant’s execution...what further showing does the Fourth Amendment require before the government may be authorized to compel the use of an individual’s biometric features in an attempt to unlock a digital device that it is authorized to search pursuant to a warrant?” *Id.* at 530. He believed “the standard should focus on the government’s evidence of the connection between the individual and the device.” *Id.* He ultimately ruled that any request to compel a person to unlock a device with a biometric must satisfy *Hayes*, meaning law enforcement must have reasonable suspicion the suspect committed the crime that is the subject matter of the warrant, and reasonable suspicion the individual’s biometric will unlock the device. *Id.* at 532-33. He settled on the reasonable suspicion standard because he believed “the privacy interest at issue here is not in the contents of the phone, but in the fingerprints or other biometric features the government seeks to use.” *Id.* at 532 n. 6.

But the issue *is* in the contents of the phone; as explained in more detail below, the government is not seeking the fingerprint its own sake, but rather to access the breadth of personal, private information stored on the device. Thus, the approaches of Judges Westmore and Weisman—requiring probable cause of a connection between a specific suspect and a specified electronic device connected to criminal activity—adequately protects the heightened privacy interests implicated by the immense amounts of personal information on an electronic device.

3. Requests for “Any Individual” at the Premises of a Search to Provide Biometrics to Unlock “Any” Unspecified Devices Are Not Particularized.

Requiring a probable cause connection between a specific suspect and a specified electronic device containing evidence of criminal activity also ensures the warrant is constitutionally particularized.

One of the “distinct constitutional protections served by the warrant requirement” is that “those searches deemed necessary should be as limited as possible.” *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). The Fourth Amendment limits searches and seizures to “specific areas and things for which there is probable cause to search.” *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). A “search [must] be carefully tailored to its justifications, and [can] not take on the character of the wide-ranging explanatory searches the Framers intended to prohibit.” *Id.*

4th & 5th Amendment Implications of Compelled Biometric Unlocking
 August 9, 2019
 Page 7

The particularity requirement is context-dependent, and the specificity required for a warrant will vary based on the amount of information available and the scope of the search to be executed. When assessing the validity of a requested search warrant, “[o]ne of the crucial factors to be considered is the information available to the government.” *United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982); *see also Garrison*, 480 U.S. at 85-86 (officers who know they do not have probable cause to search a place are “plainly” obligated to exclude it from a warrant request). “Generic classifications in a warrant are acceptable only when a more precise description is not possible.” *Cardwell*, 680 F.2d at 78 (quotations and citations omitted)). Moreover, for seizures of “innocuous” objects like cell phones—as opposed to contraband like drugs or illegal weapons—“judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.” *Andresen v. Maryland*, 427 U.S. 463, 482 n. 11(1976); *accord Griffith*, 867 F.3d at 1276.

Requests that “any” person at the premises of the search be compelled to provide biometrics to unlock “any” device found at the premises fail the particularity requirement. The Supreme Court has long held that probable cause to search an item in one location does not empower the government to search other nearby locations without a probable cause showing to that specific location. *See Walter v. United States*, 447 U.S. 649, 656-57 (1980) (“a warrant to search for a stolen refrigerator would not authorize the opening of desk drawers.”). Rather, “a search or seizure of a person must be supported by probable cause particularized with respect to that person. This requirement cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to . . . search the premises where the person may happen to be.” *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979).

That same logic necessarily extends to electronic devices. As Judge Westmore explained, the “government cannot be permitted to search and seize a mobile phone or other device that is on a non-suspect’s person simply because they are present during an otherwise lawful search.” *Matter of Residence in Oakland*, 354 F. Supp. 3d at 1014. Thus, broad requests for “any” individual to provide a biometric to unlock “any” device are unconstitutional.⁴

B. The Fifth Amendment

The Fifth Amendment states, in part, “No person... shall be compelled in any criminal case to be a witness against himself.” U.S. CONST. AMEND. V. The privilege against self-incrimination is

⁴ Requiring the government to meet the standard described above—show probable cause both that a specified electronic device is contraband or contains evidence of a crime and belongs to a specific suspect before that person can be compelled to unlock the device with biometrics—is not judicial interference with the execution of the search warrant. *See Dalia v. United States*, 441 U.S. 238, 257 (1979) (“it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant”). Once the government satisfies the legal standard, the actual process by which the biometric is compelled is up to the executing officers, subject to the Fourth Amendment’s requirement the government act reasonably. The requirements of probable cause and particularity go to whether the police can search or seize at all. When it comes to those decisions, the Fourth Amendment requires “nothing [be] left to the discretion of the officer executing the warrant.” *Marron v. United States*, 275 U.S. 192, 196 (1927).

4th & 5th Amendment Implications of Compelled Biometric Unlocking
 August 9, 2019
 Page 8

“a prohibition of the use of physical or moral compulsion to extort communications” from an individual. *Holt v. United States*, 218 U.S. 245, 253 (1910).

Fifth Amendment protection requires three things: (1) compulsion; (2) incrimination; and (3) testimony. See *Hiibel v. Sixth Judicial Dist. Court of Nevada, Humboldt Cty.*, 542 U.S. 177, 189 (2004). Compulsion occurs when the government “threaten[s] to inflict potent sanctions unless the constitutional privilege is surrendered.” *Lefkowitz v. Cunningham*, 431 U.S. 801, 805 (1977). A statement is incriminating if the answer either supports a conviction in a federal criminal case, or provides a “link in the chain of evidence” leading to incriminating evidence, even if the statement itself is not incriminating. *United States v. Hubbell*, 530 U.S. 27, 38 (2000) (quotations and citation omitted). Testimony includes the act of speaking words from a person’s mouth, which “make extensive use of the contents of his own mind.” *Id.* at 36 (internal quotations and citation omitted). Producing documents can also be testimonial because such production has “communicative aspects of its own, wholly aside from the contents of the papers produced,” as production “tacitly concedes the existence of the papers demanded and their possession or control” by the suspect. *Fisher v. United States*, 425 U.S. 391, 410 (1976).

1. Compelling a Person to Use a Biometric to Unlock an Electronic Device is “Testimonial” Because it Communicates the Existence, Authenticity, Possession and Control of Data on the Device.

Compelling a person to do a mere physical act that does not force them to use the contents of their mind is not testimonial. *Hubbell*, 530 U.S. at 43. The Fifth Amendment “offers no protection against compulsion to submit to fingerprinting, photographing, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture.” *Schmerber v. California*, 384 U.S. 757, 764 (1966). “The privilege is a bar against compelling ‘communications’ or ‘testimony,’ but that compulsion which makes a suspect or accused the source of ‘real or physical evidence’ does not violate it.” *Id.*

On the other hand, “the Fifth Amendment privilege against self-incrimination applies to acts that imply assertions of facts.” *Doe v. United States*, 487 U.S. 201, 209 (1988). Thus, “the assembly of documents” in response to a government demand is “like telling an inquisitor the combination to a wall safe.” *Hubbell*, 530 U.S. at 43.

Compelling a person to use a biometric to unlock an electronic device in the course of a criminal investigation is clearly “testimonial” because it is an act “that imply assertions of facts,” specifically that the person has dominion and control over the electronic device and its contents. *Doe*, 487 U.S. at 209. It is identical to “the assembly of documents” that tell the government “the combination to a wall safe.” *Hubbell*, 530 U.S. at 43. By unlocking a device, a person “tacitly concedes the existence of the [information] demanded and their possession or control,” which is a Fifth Amendment concern. *Fisher*, 425 U.S. at 410.⁵ “With a touch of a finger, a

⁵ Unlocking a device with a biometric is arguably greater proof of dominion and control over the device than merely knowing the password. Passwords can be shared, are freely given and easily guessed. People may know the passwords of devices that do not in fact belong to them. But biometrics are inherently more private. Biometrics are generally exclusive to one person. Some devices, such as Apple iPhones and iPads, allows users to store more than

4th & 5th Amendment Implications of Compelled Biometric Unlocking
 August 9, 2019
 Page 9

suspect is testifying that he or she has accessed the phone before, at a minimum, to set up the fingerprint password capabilities, and that he or she currently has some level of control over or relatively significant connection to the phone and its contents.” *In re Application for a Search Warrant*, 236 F. Supp. 3d at 1073.⁶

Much of the discussion about the Fifth Amendment implications of compelling a suspect to unlock an electronic device focuses on the distinction between an alphanumeric password and a biometric. A consensus has emerged that the Fifth Amendment protects a person from being forced to provide their password to law enforcement, as that requires “extensive use of the contents of his own mind.” *Hubbell*, 530 U.S. at 36; *see United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (quashing “subpoena requiring Defendant to testify—giving up his password—thereby protecting his invocation of his Fifth Amendment privilege against compelled self-incrimination.”); *United States v. Spencer*, 2018 WL 1964588, *2 (N.D. Cal. Apr. 26, 2018) (“the government could not compel Spencer to state the password itself, whether orally or in writing”); *SEC v. Huang*, 2015 WL 5611644, *3 (E.D. Penn. Sep. 23, 2015) (“Defendants’ confidential passcodes [to smartphones] are personal in nature and Defendants may properly invoke the Fifth Amendment privilege to avoid production of the passcodes”); *Matter of Decryption of a Seized Data Storage System*, 2013 WL 12327372, *4 (E.D. Wis. Apr. 19, 2013) (concluding suspect’s “act of production, which would necessarily require his using a password of some type to decrypt the storage device,” protected by Fifth Amendment).

Some courts, however, have found unlocking an electronic device with a biometric unprotected by the Fifth Amendment because supplying a fingerprint is merely a physical act with no communication at all. These cases equate the act of using a biometric to unlock the device with “the government’s compelled use of other ‘physical characteristics’ of criminal suspects that courts have found non-testimonial even when they are used for investigatory purposes rather than solely for identification.” *Matter of Search of [Redacted] Washington, D.C.*, 317 F. Supp. 3d at 536; *see also Matter of Search Warrant Application for [redacted text]*, 279 F. Supp. 3d

one biometric on the device. *See* “Use Touch ID on iPhone and iPad,” Apple Support, *available at* <https://support.apple.com/en-us/HT201371> (“Enroll up to five fingerprints.”) (last visited August 9, 2019). But storing five fingerprints does not mean five people have access to the device; one person can enroll all the fingers on one hand, some combination of fingers on both hands, or allow five separate people enroll their fingerprint on the device. Regardless, significantly fewer people will have access to a device locked with a biometric than an alphanumeric password.

⁶ Unlocking the device will also typically decrypt the device, as many electronic devices, including Apple iPhones and iPads, and Google’s Nexus and Pixel Android phones, are encrypted by default. *See* “Our Approach to Privacy,” Apple, *available at* <https://www.apple.com/privacy/approach-to-privacy/> (“We were one of the first companies to automatically include native operating system-supported disk encryption with FileVault in macOS and data protection in iOS.”) (last visited August 9, 2019); “Encrypt your Data,” Google Nexus Help, *available at* <https://support.google.com/nexus/answer/2844831> (“All Pixel phones are encrypted by default. So are Nexus 5X, Nexus 6P, Nexus 6 and Nexus 9 devices.”) (last visited August 9, 2019). The act of decryption is itself a separate communication, translating otherwise unintelligible data into a form that can be used and understood by law enforcement.

4th & 5th Amendment Implications of Compelled Biometric Unlocking
 August 9, 2019
 Page 10

800, 805 (N.D. Ill. 2017) (unlocking electronic device with a biometric merely providing “a physical characteristic of some sort.”).

But that approach puts form over substance and has been rejected by the only federal appeals court to consider the issue, the Eleventh Circuit in *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012).⁷ There, the government issued a grand jury subpoena directing a suspect to provide the unencrypted contents of a computer that law enforcement had lawfully seized pursuant to a warrant but were unable to decrypt. 670 F.3d at 1339. The Eleventh Circuit held the Fifth Amendment privilege applied to the act of providing the decrypted contents of the computer. The government argued it did not seek “the combination or the key” to the computer, “but rather the contents” contained inside. *Id.* at 1346.⁸ The Eleventh Circuit found this “argument badly misses the mark.” *Id.* It noted in the pertinent Supreme Court cases, “the government never sought the ‘key’ or the ‘combination’ to the safe for its own sake; rather, the government sought the files being withheld, just as the government does here.” *Id.* (citing *Hubbell*, 530 U.S. at 38; *Fisher*, 425 U.S. at 394-95). In that circumstance, requiring a person to provide the decrypted contents of the computer “is most certainly more akin to requiring the production of a combination because both demand the use of the contents of the mind, and the production is accompanied by the implied factual statements noted above that could prove to be incriminatory.” *Id.*

The same is true here. The government is not seeking the fingerprint merely for the sake of having a fingerprint; it seeks the fingerprint to unlock an electronic device and get access to the data contained inside. The Supreme Court in *Schmerber* itself noted that compelling a person to provide physical evidence that “makes a suspect or accused the source of ‘real or physical evidence’ does not violate” the Fifth Amendment. 384 U.S. at 764 (emphasis added). But in the case of biometrics, the suspect’s fingerprint is not “the source of ‘real or physical evidence’” the government seeks. The fingerprint is a combination to the safe—the electronic device—stuffed with reams of personal data that is “real or physical evidence” sought by the government. An act that results in a tacit admission of dominion and control over the safe and the documents therein,

⁷ In any event, a password is a necessary prerequisite to using a biometric. Apple’s Touch ID, which allows an iPhone or iPad to be unlocked with a fingerprint, requires a user create an alphanumeric password. See “Use Touch ID on iPhone and iPad,” Apple Support, available at <https://support.apple.com/en-us/HT201371> (“Before you can set up Touch ID, you need to create a password for your device.”) (last visited August 9, 2019).

⁸ Many Fifth Amendment cases use an example from Justice Stevens’ dissenting opinion in *Doe*, distinguishing between a person forced to surrender a physical key to a locked box containing incriminating documents—which is deemed non-testimonial—and being compelled to reveal the combination of a wall safe—which is testimonial. See *Doe*, 487 U.S. at 219 (Stevens, J., dissenting). But as one state court recently noted, “despite the many cases referencing the quote, we have found none that provide details of ‘surrender[ing] a key.’ We question whether identifying the key which will open the strongbox—such that the key is surrendered—is, in fact, distinct from telling an officer the combination. More importantly, we question the continuing viability of any distinction as technology advances.” *State v. Stahl*, 206 So. 3d 124, 134–35 (Fla. Dist. Ct. App. 2016). We agree; the distinction between a safe and a key is irrelevant particularly in the 21st century. What matters is whether a person is being compelled to do an act that communicates the person has dominion and control over items sought by law enforcement that will result in the production of potentially incriminating evidence to law enforcement.

4th & 5th Amendment Implications of Compelled Biometric Unlocking
 August 9, 2019
 Page 11

and that will result in the production of those documents to the government, is clearly testimonial under the Fifth Amendment.

Moreover, equating a biometric used to unlock an electronic device with merely obtaining a physical fingerprint ignores the Supreme Court's repeated admonitions that ensuring constitutional protections are not "at the mercy of advancing technology" requires adoption of rules that "take account of more sophisticated systems that are already in use or in development." *Kyllo*, 533 U.S. at 35. Even in the Fifth Amendment context itself, the Supreme Court warned in *Fisher* that questions about whether an act is testimonial "do not lend themselves to categorical answers; their resolution may instead depend on the facts and circumstances of particular cases or classes thereof." 425 U.S. at 410. The Court presciently warned that there may be "special problems of privacy" with trying to compel a person to produce "a personal diary" or a request that implicates "First Amendment values." *Id.* at 401 n. 7.

As Judge Westmore explained earlier this year, unlocking a digital device with a biometric "is fundamentally different than requiring a suspect to submit to fingerprinting" and "far exceeds the 'physical evidence' created when a suspect submits to fingerprinting to merely compare his fingerprints to existing physical evidence (another fingerprint) found at a crime scene." *Matter of Residence in Oakland, California*, 354 F. Supp. 3d at 1016. Given the breadth of personal and private information on an electronic device sought by police, compelling a person use a biometric to unlock the device is "testimonial" under the Fifth Amendment.

2. The "Foregone Conclusion" Doctrine Requires the Government Demonstrate with "Reasonable Particularity" Specific Data it Seeks Exists in a Specified Location, is Possessed by the Target and is Authentic.

In *Fisher*, the Supreme Court explained the Fifth Amendment privilege does not apply if "the existence and location of the papers are a foregone conclusion," and the suspect "adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers." 425 U.S. at 411. In that scenario, "the question is not of testimony but of surrender." *Id.* (quotations and citation omitted). The government bears the burden of proving this "foregone conclusion" exception applies based on the "information possessed by the government *before* it" made the demand. *In re Grand Jury Subpoena, Dated April 18, 2003*, 383 F.3d 905, 910 (9th Cir. 2004) (emphasis in original) (citations and quotations omitted). The government must establish "reasonable particularity" that the documents exist and the person possesses them before the doctrine applies and production is deemed non-testimonial. *Id.*

In the context of an electronic device, the Eleventh Circuit has adopted the Ninth Circuit's standard and explained the government could only satisfy the "foregone conclusion" if it shows with "reasonable particularity that it seeks a certain file and is aware, based on other information, that (1) the file exists in some specified location, (2) the file is possessed by the target of the subpoena, and (3) the file is authentic." *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d at 1349 n. 28; *see also id.* at 1344 n. 20 (noting it was "persuaded by the[] reasoning" of *In re Grand Jury Subpoena, Dated April 18, 2003* and "now follow suit").

4th & 5th Amendment Implications of Compelled Biometric Unlocking
 August 9, 2019
 Page 12

The key to the doctrine is specificity; the government must “establish that a file or account, whatever its label, does in fact exist” on the device and the suspect can access it. *Id.* The mere knowledge that a person can unlock the device is insufficient. *See Huang*, 2015 WL 5611644, at *3 (“Merely possessing the smartphones is insufficient if the SEC cannot show what is actually on the device.”). Nor will “categorical requests for documents the Government anticipates are likely to exist...suffice.” *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d at 1347. The Supreme Court explained in *Hubbell* the government could not cure the “deficiency” of not having “prior knowledge of either the existence of the whereabouts” of compelled documents “through the overbroad argument that a businessman such as respondent will always possess general business and tax records that fall within the broad categories described in this subpoena.” 530 U.S. at 45.

The cases applying the foregone conclusion doctrine to the act of unlocking or decrypting an electronic device all involved specific and detailed knowledge by the government of the data it sought prior to its effort to compel decryption. For example, the doctrine applied in *United States v. Apple MacPro Computer* when prior to compelling a suspect to decrypt a computer, police found child pornography on that same computer, logs showing that computer had visited child exploitation websites, hash values on that computer matched known child pornography images, and the suspect’s sister told police the suspect had unlocked the same computer to show her child pornography. 851 F.3d 238, 242-43 (3d Cir. 2017). In *In re Boucher*, the foregone conclusion doctrine applied when the defendant admitted he had downloaded child pornography and officers personally observed thousands of file names reflecting child pornography on a computer before they sought to compel him to decrypt that same device. 2009 WL 424718, *2 (D. Vt. Nov. 29, 2009).

Due to the need for specificity, it is doubtful the “foregone conclusion” doctrine would ever extend to overbroad requests to compel biometrics of “any” person or “any” electronic device at the premises of a search. As Judge Westmore noted, the government “would be unable to articulate facts to compel the unlocking of devices using biometric features by unknown persons the Government could not possibly anticipate being present during the execution of the search warrant.” *Matter of Residence in Oakland, California*, 354 F. Supp. 3d at 1018.

3. The Only Way to Overcome the Fifth Amendment Privilege is for the Government to Offer Use and Derivative Use Immunity.

Determining the Fifth Amendment privilege against self-incrimination applies to the act of compelling an individual to provide their biometric to unlock an electronic device is not the end of the inquiry. The government does have the “right to every man’s evidence” and may compel testimony. *Kastigar v. United States*, 406 U.S. 441, 443 (1972). The “rational accommodation between the imperatives of the privilege and the legitimate demands of government to compel citizens to testify” has been the use of immunity. *Id.* at 446. Any grant of “immunity” must be “coextensive with the scope of the privilege.” *Id.* at 449.

The federal immunity statute, 18 U.S.C. § 6002, states a witness may not refuse to testify on “the basis of his privilege against self-incrimination,” but that “no testimony or other information compelled under the order (or any information directly or indirectly derived from such testimony

4th & 5th Amendment Implications of Compelled Biometric Unlocking
August 9, 2019
Page 13

or other information) may be used against the witness in any criminal case” except in prosecutions for perjury, making a false statement or failing to comply with the order. *Kastigar* held that § 6002 is “coextensive” with the Fifth Amendment because it provides “immunity from the use of compelled testimony and evidence derived therefrom.” 406 U.S. at 452-53.

As the Eleventh Circuit explained, in order to provide immunity “coextensive” with the Fifth Amendment, a government demand that a suspect use a biometric to unlock an electronic device must be accompanied by an offer of use and derivative use immunity. *See In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d at 1351-52. “The government cannot obtain immunity only for the act of production and then seek to introduce the contents of the production, regardless of whether those contents are characterized as nontestimonial evidence, because doing so would allow the use of evidence derived from the original testimonial statement.” *Id.* at 1351. Thus, the government must provide immunity for the act of production—supplying the biometric that unlocks the electronic device and provides law enforcement with the data it seeks—and refrain from introducing any evidence it obtains from the electronic device in a criminal proceeding against the compelled suspect. Absent such a grant of immunity, the Fifth Amendment prohibits a person from being compelled to provide their biometric to unlock an electronic device.

Again Your Honor, the Federal Public Defender appreciates the opportunity to provide our position on this critical, fast-developing legal issue. If the office can be of any further assistance on this specific issue, or any other issues that arise before the Court, please do not hesitate to let us know.

Sincerely,-

STEVEN G. KALAR
Federal Public Defender
Northern District of California



HANNI M. FAKHOURY
Assistant Federal Public Defender

CC: Steven G. Kalar, Federal Public Defender
Varell Fuller, Supervising Attorney, San Jose Branch